(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2000－516313
（P2000－516313A）
(43)公表日　平成12年12月５日(2000.12.5)

(51)Int.Cl.[6]	識別記号	ＦＩ		テーマコード（参考）
Ｅ０５Ｂ　49/00		Ｅ０５Ｂ	49/00	Ｋ
Ｈ０４Ｑ　9/00	３０１	Ｈ０４Ｑ	9/00	３０１Ｂ
	３１１			３１１Ｑ
// Ｈ０４Ｌ　9/32		Ｈ０４Ｌ	9/00	６７３Ｂ

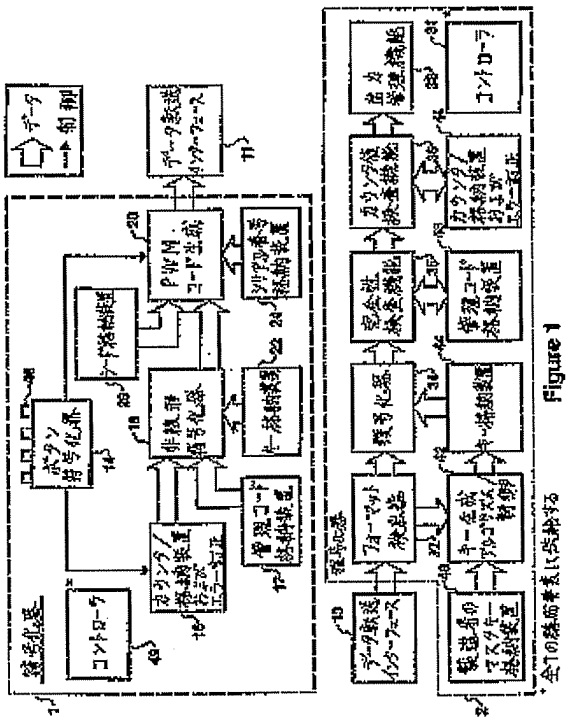
審査請求　未請求　予備審査請求　未請求(全 48 頁)

(21)出願番号　特願平11－502790
(86)(22)出願日　平成10年６月３日(1998.6.3)
(85)翻訳文提出日　平成11年１月29日(1999.1.29)
(86)国際出願番号　ＰＣＴ／ＵＳ９８／１１３６５
(87)国際公開番号　ＷＯ９８／５５７１７
(87)国際公開日　平成10年12月10日(1998.12.10)
(31)優先権主張番号　０８／８６８，１３１
(32)優先日　平成９年６月３日(1997.6.3)
(33)優先権主張国　米国（US）
(81)指定国　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＪＰ，ＫＲ

(71)出願人　マイクロチップ　テクノロジー　インコーポレイテッド
アメリカ合衆国　アリゾナ　85224－6199，チャンドラー，ウェスト　チャンドラー　ブールバード　2355
(72)発明者　ブルワー，フレデリック　ジェイ．
南アフリカ国　リトルトン　0140，クリフトン　アベニュー，ライフスタイル　マネジメント　パーク，ユニット　ナンバー　2（番地なし）
(74)代理人　弁理士　山本　秀策

(54)【発明の名称】　改良された安全な自己学習システム

(57)【要約】
安全な自己学習能力を有するデバイスのリモートコントロールのための方法およびシステム。システムは、符号化器および復号化器を有し、符号化器は、ユーザキーを含む変数情報を、非線形アルゴリズムを用いて符号化し、復号化器に送信される符号化値を生成し、復号化器は、同じアルゴリズムを用いて値を復号化する。学習モードにおいて、新しい符号化器は、システムに付加される。新しい符号化器は、キー生成シードを用いて符号化値を生成する。復号化器は、符号化されたキー生成シードを受信すると、復号化されたキー生成シードに基づいて復号化キーを生成する。復号化キーは、新しい符号化器の有効な認識を安全に可能にする復号化器のメモリに格納される。



【特許請求の範囲】

1．符号化器と、学習モード起動手段と、復号化器とを有するアクセス制御システムであって、該符号化器は、

シリアル番号を格納する手段と、

シード、ならびに製造者のマスタキーと該シードおよび該シリアル番号のうちの少なくとも1つとを用いて生成される第1のキーのうちの少なくとも1つを格納する手段と、

少なくとも、該シード、該シリアル番号、ならびに該第1のキーおよびアルゴリズムを入力値に適用することによって得られる情報から選択されるキー生成情報を含む信号を転送する手段とを有し、

該復号化器を学習モードに設定する復号化器学習モード起動手段は、該符号化器および該復号化器から物理的に離れており、

該復号化器は、製造者のマスタキーを格納する手段と、

該転送された信号を受信する手段と、

少なくとも、該キー生成情報および該製造者のマスタキーを用いて第2のキーを生成する手段とを有する、アクセス制御システム。

2．符号化器および復号化器を有するアクセス制御システムを作動する方法であって、

シリアル番号を格納するステップと、

シード、ならびに製造者のマスタキーと該シードおよび該シリアル番号のうちの少なくとも1つとを用いて生成される第1のキーのうちの少なくとも1つを格納するステップと、

該符号化器を用いて、少なくとも、該シード、該シリアル番号、ならびに該第1のキーおよびアルゴリズムを入力値に適用することによって得られる情報から選択されるキー生成情報を含む信号を転送するステップと、

製造者のマスタキーを該復号化器に格納するステップと、

該復号化器を学習モードに設定する復号化器学習モード起動手段を起動するステップであって、該手段が該符号化器および該復号化器から離れている、ステップ

プと、

該転送された信号を該復号化器によって受信するステップと、

少なくとも、該キー生成情報および該製造者のマスタキーを用いて、該復号化器によって第２のキーを生成するステップとを包含する方法。

３．製造者のマスタキーを格納するステップと、

復号化器から物理的に離れたまたは分離された復号化器学習モード起動手段を起動することによって該復号化器を学習モードに設定するステップと、

少なくとも、シード、シリアル番号、ならびに第１のキーおよびアルゴリズムを入力値に適用することによって得られる符号化された情報から選択されるキー生成情報を含む信号を受信するステップと、

少なくとも、該キー生成情報および該製造者のマスタキーを用いて第２のキーを生成するステップと、

を包含する復号化器を作動する方法。

４．符号化器および復号化器を有する改良されたローリングコードまたはコードホッピングシステムであって、該改良が、

復号化器学習モード起動手段を有し、該手段が起動されると、該復号化器は学習モードに設定され、該手段は該符号化器および該復号化器から物理的に離れるかまたは分離されている、ローリングコードまたはコードホッピングシステム。

５．送信機および受信機を有する改良されたコードホッピングまたはローリングコードシステムであって、該改良が、

受信機学習モードスイッチを有し、該スイッチが起動されると、該受信機は学習モードに設定され、該スイッチは該受信機および該送信機から物理的に分離または離れている、コードホッピングまたはローリングコードシステム。

【発明の詳細な説明】

改良された安全な自己学習システム

本願は、１９９４年９月３０日出願の出願シリアル番号第０８／３１３，６１３号の一部継続出願である。本明細書において、上記出願の開示を参考として援用する。上記出願は、１９９２年１２月４日出願の出願シリアル番号第０７／９８５，９２９号の一部継続出願である。本明細書において、上記出願の開示を参考として援用する。上記出願は、現在は放棄されている１９９１年５月２９日出願の出願シリアル番号第０７／７０７，１０１号の一部継続出願である。

１．発明の分野

本発明は、改良された安全な自己学習システムおよびその方法に関し、具体的には、改良された安全な自己学習システム、ならびにセキュリティシステムにおけるシステムおよび装置をリモートコントロールする方法に関する。

２．背景の説明

超音波、高周波、または赤外トランスデューサを介するシステムまたは装置のリモートコントロールは、建築物および乗り物のためのセキュリティシステム、リモートコントロール式のガレージのドアおよびゲートオープナーなどの多くのアプリケーションにおいて普及している。現在使用されているある一方向送信システムは、セキュリティの面で、以下の非常に重要な２つの欠点を有する。即ち、（ａ）一方向送信システムが送信するコードが通常固定されていること、および（ｂ）コードの可能な組み合わせの数が比較的少ないことである。これらの欠点のいずれも、認証されないアクセスにつながり得る。

ほとんどのリモートコントロールシステムにおいて利用可能である可能な組み合わせの数は制限されているため、比較的短時間にすべての可能な組み合わせを送信することが可能である。この目的のための携帯型のマイクロプロセッサベースのシステム（コードスキャナと呼ばれる）は、容易に構成され得る。

８つのＤＩＰスイッチを用いるシステム（２５６個の組み合わせ）では、この走査プロセスは、１秒あたり８つの組み合わせを試みる場合、典型的には、３２秒未満で達成され得る。６５，５３６個の組み合わせを生じる、１６ビットのキ

ーを用いるシステムであっても、すべての可能な組み合わせを試みるために２１／４時間しか必要とされない。また、スキャナは、この最大時間よりもはるかに少ない時間でアクセスを獲得し得、平均時間は、実際には、合計時間の半分である。

セキュリティシステムへの認証されないアクセスを獲得するためのより容易な方法が自由に利用可能である。このタイプのユニットは、「乗り物の合法的な回収」のための道具として広告されている。乗り物のセキュリティおよびリモートコントロールシステムにおいて通常使用されるタイプのリモートコントロール送信機は、特定の周波数でコード番号を送信する小型の無線送信機を含む。このコード番号は通常、集積回路符号化器によって生成される。この送信周波数は通常、特定の国内で法律によって固定されている。従って、そのような送信機のすべてから信号を受信することができる受信機を作り、これを、受信機により捕獲される送信を記録する回路とともに使用することが可能である。そのような装置は、コードまたはキーグラバとして知られており、リモートコントロールセキュリティシステムを用いて、保護された構内へのアクセス、または乗り物へのアクセスを獲得するために使用され得る。

固定コードシステムの制限を克服するために、コードホッピングおよびローリングコードシステムが、現在利用可能である（ＺＡ特許第９１／４０６３号および米国特許第５，１０３，２２１号参照）。上記特許の明細書は、アルゴリズムを使用して、送信機が起動される度に異なる送信を生成する送信機を記載している。コードが受信され復号化されると、復号化器は、有効な送信が行われた場合にのみ応答する。格納されたキーとともに、特殊なアルゴリズムを使用して、符号化された受信を復号化する場合もある（ＺＡ特許第９１／４０６３号参照）。その後、復号化された値は、格納された値と比較され、送信が合法であるかどうかが判定される。

コードホッピングおよびローリングコードシステムの欠点は、失われた、盗まれた、または使用できなくなった送信機を取り替えるまたは不能にすることが困難であることである。製造者または販売者により、外部の機器を使用して、送信

機をプログラムし直すかまたは取り替えなければならない。このプロセスの間に、セキュリティ上の問題点が生じ得る。

理想的には、セキュリティシステムは、ユーザがシステムに新しい送信機を追加するかまたは送信機を取り替えることを必要とする場合に、販売者の介入を必要としてはならない。ユーザは、一般の取り替え用送信機をいつでもすぐに購入することができ、且つ、この送信機を、都合の良いときに、助けなしで追加することができなければならない。学習システムは、復号化器が、特殊な機器を用いて外部からプログラムし直す必要なく、新しい送信機のアイデンティティを「学習」するという点で、この能力を提供する。

しかし、学習システムは、ユーザがシステムに新しい送信機を追加することを可能にしなければならないだけではなく、前の送信機が権限のない人物の手に渡る可能性があるため、前の送信機をシステムから排除する手段を有していなければならない。

自己学習固定コードシステムでは、入力されるコードは、システムが学習モードである場合、復号化器によって将来の参照のために格納される。その後の送信は、学習されたコードと比較される。新しい送信機コードを学習するための異なる構成が使用される。復号化器を通常動作モードまたは学習モードのいずれかに設定するために、スイッチが使用され得る（米国特許第４，７５０，１１８号および同第４，９１２，４６３号）。学習モードでは、復号化器は、送信機からの新しい有効なコードを学習することができる。同様の手段が、復号化器を、新しい送信機コードに反応するようにプログラムするために使用される（米国特許第４，９３１，７８９号および同第５，０４９，８６７号参照）。別の特許（米国特許第５，１４８，１５９参照）では、復号化器により、ランダムに選択された固定コードが生成され、関連する送信機にプログラムされる。米国特許第４，８５５，７１３号は、携帯型プログラマを使用して、復号化器により認識される新しい固定コードをプログラムすることを記載している。上記特許のすべてにおいて、送信またはプログラムされたコードは、格納された固定コードである。使用される学習機構に拘わらず、依然として、コードのグラビング（grabbing）また

はコード生成によるセキュリティ上の脅威が存在する。さらに、これらのシステムが学習するためには、（1）ユーザは、扱いにくく、より高価な2スイッチシステムを使用しなければならない、および／または（2）ユーザは、（a）例えばガレージドア開放システムの受信機などのシステムが、一旦、例えばユーザのガレージの天井などに設置されると、起動させることが（年配者または障害者にとっては、不可能ではないにしても）非常に困難となり得る受信機／復号化器に物理的に不便に配置されるスイッチ（米国特許第4，750，118号の図1参照）、（b）起動および使用が複雑であり得る送信機であって、送信機が失われた場合もしくはさらに悪い場合には盗まれた場合に安全でない可能性のある送信機によって送られるコード、または（c）使用が複雑であり得る別個のプログラミング手段であって、同様に、プログラミング手段が失われた場合もしくはさらに悪い場合には盗まれた場合に安全でない可能性のあるプログラミング手段によって送られるコード、を介して、受信機／復号化器を学習モードに設定しなければならない。

以下の米国特許、第RE29，525号、第4，380，762号、第4，385，296号、第4，426，637号、第4，529，980号、第4，534，333号、第4，574，247号、第4，590，470号、第4，596，985号、第4，638，433号、第4，652，860号、第4，686，529号、第4，737，770号、第4，779，090号、第4，835，407号、第4，847，614号、第4，855，713号、第4，878，052号、第4，890，108号、第4，928，098号、第4，951，029号、第4，988，992号、第5，049，856号、および第5，055，701号の明細書もまた、参照されたい。

上述の固定コードシステムとは異なり、本願の発明は、安全な自己学習コードホッピングまたはローリングコードシステムを提供し、これにより、コードグラビング装置またはコード生成装置によるセキュリティ上の脅威が取り除かれる。

1つの好ましい実施態様によると、本願の発明は、符号化器および復号化器を有する改良されたローリングコードまたはコードホッピングシステムであって、

改良が、復号化器学習モード起動手段を有し、手段が起動されると、復号化器は学習モードに設定され、手段は符号化器および復号化器、ならびに好ましくは他のすべてのプログラミング手段から物理的に離れるかまたは分離されている、ローリングコードまたはコードホッピングシステムを提供する。

他の実施態様によると、本願発明は、送信機および受信機を有する改良されたコードホッピングまたはローリングコードシステムであって、改良が、受信機学習モードスイッチを有し、スイッチが起動されると、受信機は学習モードに設定され、スイッチは受信機および送信機、ならびに好ましくは他のすべてのプログラミング手段から物理的に分離または離れている、コードホッピングまたはローリングコードシステムを提供する。

本発明は、第一に、

シリアル番号を格納するステップと、

シード、ならびに製造者のマスタキーとシードおよびシリアル番号のうちの少なくとも1つとを用いて生成されるキーのうちの少なくとも1つを格納するステップと、

少なくとも、シード、シリアル番号、ならびにキーおよびアルゴリズムを入力値に適用することによって得られる情報から選択されるキー生成情報を転送するステップとを有する符号化器を動作する方法を提供する。

入力値は、少なくとも、管理コード、カウンタ値、およびコマンドに関連する情報から選択される情報を含み得る。

1つの実施態様において、方法は、

各パラメータセットが、少なくとも、それぞれのシリアル番号、それぞれのシード、それぞれのキー、ならびにそれぞれのキーおよびアルゴリズムをそれぞれの入力値に適用することによって得られるそれぞれの情報から選択される情報を含む複数のパラメータセットを格納するステップと、

パラメータセットを選択するステップと、

選択されたパラメータセットに対するそれぞれのキー生成情報を転送するステップとを包含する。

各入力値は、少なくとも、それぞれの管理コード、それぞれのカウンタ値、お

よびコマンドに関連する情報から選択される情報を含み得る。

本発明はまた、製造者のマスタキーを格納するステップと、

復号化器から物理的に離れたまたは分離された復号化器学習モード起動手段を起動することによって復号化器を学習モードに設定するステップと、

少なくとも、シード、シリアル番号、ならびに第1のキーおよびアルゴリズムを入力値に適用することによって得られる符号化された情報から選択されるキー生成情報を含む信号を受信するステップと、

少なくとも、キー生成情報および製造者のマスタキーを用いて第2のキーを生成するステップとを包含する復号化器を作動する方法を提供する。

方法は、第2のキー、キー生成情報、およびシリアル番号のうちの少なくとも1つを格納するステップを含み得る。

1つの実施態様において、受信された信号は、符号化された情報を含み、方法は、

復号化アルゴリズムおよび予め生成された第2のキーを用いて符号化された情報を復号化し、それにより、少なくとも、管理コード、カウンタ値、およびコマンドに関連する情報から選択される情報を含む復号化された入力値を得るステップと、

復号化された入力値を格納するステップとを包含する。

方法は、各パラメータセットが、少なくともそれぞれのシリアル番号、それぞれの管理コード、およびそれぞれのカウンタ値から選択される情報を含む、複数のパラメータセットを格納するステップを含み得る。

本発明はさらに、符号化器および復号化器を有するアクセス制御システムを作動する方法であって、

シリアル番号を格納するステップと、

シード、ならびに製造者のマスタキーとシードおよびシリアル番号のうちの少なくとも1つとを用いて生成される第1のキーのうちの少なくとも1つを格納するステップと、

符号化器を用いて、少なくとも、シード、シリアル番号、ならびに第1のキーおよびアルゴリズムを入力値に適用することによって得られる情報から選択され

るキー生成情報を含む信号を転送するステップと、

製造者のマスタキーを復号化器に格納するステップと、

復号化器を学習モードに設定する復号化器学習モード起動手段を起動するステップであって、手段が符号化器および復号化器から離れている、ステップと、

転送された信号を復号化器によって受信するステップと、

少なくともキー生成情報および製造者のマスタキーを用いて、復号化器によって第2のキーを生成するステップとを包含する方法を提供する。

第2のキーまたはキー生成情報は格納され得る。前者の場合、方法は、

コマンドを用いて符号化器を起動するステップと、

第1のキーおよびアルゴリズムを用いて少なくとも入力値を符号化し、符号化された部分を形成するステップであって、入力値は、少なくとも、カウンタ値、管理コード、およびコマンドに関連する情報から選択される情報を含む、ステップと、

符号化器を用いて、少なくとも、シリアル番号および符号化された部分から形成される信号を転送するステップとを包含し、復号化器において、

転送された信号を受信するステップと、

第2のキーおよび復号化アルゴリズムを用いて、転送された信号における符号化された部分を復号化して入力値を得るステップとを包含する。

後者の場合において、方法は、

コマンドを用いて符号化器を起動するステップと、

第1のキーおよびアルゴリズムを用いて少なくとも入力値を符号化し、符号化された部分を形成するステップであって、入力値は、少なくとも、カウンタ値、管理コード、およびコマンドに関連する情報から選択される情報を含む、ステップと、

符号化器を用いて、少なくとも、シリアル番号および符号化された部分から形成される信号を転送するステップとを包含し、復号化器において、

転送された信号を受信するステップと、

キー生成情報および復号化アルゴリズムを用いて、転送された信号における符号化された部分を復号化して入力値を得るステップとを包含する。

方法はさらに、

符号化器において、各パラメータセットが、少なくとも、それぞれのシリアル番号、それぞれのシード、ならびにそれぞれのキーおよびアルゴリズムをそれぞれの入力値に適用することによって得られるそれぞれの情報から選択される情報を含む、複数のパラメータセットを格納するステップと、

パラメータセットを選択するステップと、

コマンドを用いて符号化器を起動するステップと、

選択されたパラメータセットに関連するキー生成情報を含む信号を転送するステップとを包含し、

復号化器において、各パラメータセットが、少なくとも、それぞれのシリアル番号、それぞれの管理コード、およびそれぞれのカウンタ値から選択される情報を含む、複数のパラメータセットを格納するステップと、

転送された信号を受信するステップと、

製造者のマスタキーおよび転送された信号に含まれるキー生成情報を用いて、選択されたパラメータセットに関連するそれぞれの第２のキーを生成するステップとを包含する。

好ましくは、符号化器および復号化器は、それぞれのマイクロチップにそれぞれ形成される。

本発明はまた、

シリアル番号を格納する手段と、

シード、ならびに製造者のマスタキーとシードおよびシリアル番号のうちの少なくとも１つとを用いて生成されるキーのうちの少なくとも１つを格納する手段と、

少なくとも、シード、シリアル番号、ならびにキーおよびアルゴリズムを入力値に適用することによって得られる情報から選択されるキー生成情報を転送する手段とを有する符号化器を提供する。

符号化器は、

各パラメータセットが、少なくとも、それぞれのシリアル番号、それぞれのシード、それぞれのキー、ならびにそれぞれのキーおよびアルゴリズムをそれぞれ

の入力値に適用することによって得られるそれぞれの情報から選択される情報を含む、複数のパラメータセットを格納する手段と、

パラメータセットを選択する手段とを含み得、

転送手段は、選択されたパラメータセットについてのそれぞれのキー生成情報を転送するように適応されている。

本発明はまた、

製造者のマスタキーを格納する手段と、

少なくとも、シード、シリアル番号、ならびに第１のキーおよびアルゴリズムを入力値に適用することによって得られる符号化された情報から選択されるキー生成情報を含む信号を受信する手段と、

少なくともキー生成情報および製造者マスタキーを用いて、第２のキーを生成する手段とを含む復号化器を提供する。

第２のキー、キー生成情報、およびシリアル番号のうちの少なくとも１つを格納するための手段が設けられ得る。

本発明はさらに、符号化器と、学習モード起動手段と、復号化器とを有するアクセス制御システムであって、符号化器は、

シリアル番号を格納する手段と、

シード、ならびに製造者のマスタキーとシードおよびシリアル番号のうちの少なくとも１つとを用いて生成される第１のキーのうちの少なくとも１つを格納する手段と、

少なくともシード、シリアル番号、ならびに第１のキーおよびアルゴリズムを入力値に適用することによって得られる情報から選択されるキー生成情報を含む信号を転送する手段とを有し、

復号化器を学習モードに設定する復号化器学習モード起動手段は、符号化器および復号化器から物理的に離れており、

復号化器は、製造者のマスタキーを格納する手段と、

転送された信号を受信する手段と、

少なくともキー生成情報および製造者のマスタキーを用いて第２のキーを生成する手段とを有する、アクセス制御システムを提供する。

システムは、第２のキーまたはキー生成情報を格納するための手段を含み得る。

前者の場合、システムは、

コマンドで符号化器を起動させるための手段と、

第１のキーおよびアルゴリズムを用いて少なくとも１つの入力値を符号化し、符号化部分を形成するための手段とを含み得、入力値は、少なくとも

カウンタ値、

管理コード、および

コマンドに関連する情報、から選択される情報を含み、

少なくともシリアル番号および符号化部分から、符号化器による転送のための信号を形成するための手段をさらに含み得、

復号化器は、第２のキーおよび復号化アルゴリズムを用いて、信号受信手段によって受信される転送された信号の符号化部分を復号化して、入力値を得るための手段を含む。

後者の場合、システムは、

コマンドで符号化器を起動させるための手段と、

第１のキーおよびアルゴリズムを用いて少なくとも入力値を符号化し、符号化部分を形成するための手段とを含み得、入力値は、少なくとも

カウンタ値、

管理コード、および

コマンドに関連する情報、から選択される情報を含み、

少なくともシリアル番号および符号化部分から、符号化器による転送のための信号を形成するための手段をさらに含み得、

復号化器は、キー生成情報および復号化アルゴリズムを用いて、信号受信手段によって受信される転送された信号の符号化部分を復号化して、入力値を得るための手段を含む。

システムは、符号化器で、パラメータの複数のセットを格納するための手段を含み得、パラメータの各セットが、少なくとも

それぞれのシリアル番号、

それぞれのシード、および

それぞれのキーおよびアルゴリズムをそれぞれの入力値に適用することによって得られるそれぞれの情報、から選択される情報を含み、

パラメータのセットを選択するための手段と、

コマンドを用いて、符号化器を起動させるための手段とをさらに含み得、

信号転送手段は、その後、選択されたパラメータのセットに関連するキー生成情報を含む信号を転送し、

復号化器で、パラメータの複数のセットを格納するための手段をさらに含み得、パラメータの各セットは、少なくとも

それぞれのシリアル番号、

それぞれの管理コード、および

それぞれのカウンタ値、から選択される情報を含み、

転送された信号に含まれるキー生成情報および製造者のマスタキーを使用して、信号受信手段によって受信される、それぞれの第2のキーを生成させて、選択されたパラメータのセットと関連させるための手段をさらに含む。

好適には、符号化器および復号化器は、それぞれのマイクロチップ内で形成される。

本発明の目的は、いわゆる「スマードカード」などのトランスミッタまたはトークンが、外部装置なしに、且つクリアなフォーマット、すなわち符号化されていない形態で符号化キーを伝送することなく、ユーザによって置換またはシステムに追加され得るアクセス制御システムを提供することである。

アクセス制御システムは、システムに対する無許可のアクセスを防止するために、復号化器において、盗まれたトランスミッタコードをディセーブルすることを可能にする。

本発明の別の目的は、コードの不正取得または走査方法の使用を防止するように起動するアクセス制御システムを提供することである。

本発明はさらに、アクセス制御システムにおいて用いられる符号化器および復号化器、並びにそれらの動作方法に関する。

製造プロセスにおいて、符号化器は、復号化器の範囲に関連する異なるシリアル番号でプログラムされる。製造業者独自のマスタキーをアルゴリズムおよびシリアル番号と共に用いて、ユーザキーを生成し、符号化器の不揮発性メモリ内に、カウンタ、管理コード、および他の情報と共に格納する。いくつかの送信を処理する（異なる入力を起動することにより異なるコマンドを送信する）ために、これらのパラメータのいくつかのセットが格納され得る。製造業者のマスターキーもまた、全ての製造業者の復号化器内に格納される。ユーザデータおよび制御データもまた、符号化器によって起動される必要のある異なる機能を制御するようにプログラムされる。符号化器内でユーザキーを生成するために用いられたものと同一のアルゴリズムが、復号化器内にも存在しなければならない。

符号化器の通常動作において、パラメータセットに関連するキー情報を用いて、専用アルゴリズムを利用することにより、変数カウンタ情報を、符号化器管理コード、シリアル番号、および他の情報と共に符号化する。符号化される情報は、符号化器が起動される度に異なる。この手法は、コードホッピングと呼ばれる。カウンタ情報が変化することは公知であるが、情報を符号化する秘密キーおよびアルゴリズムのために、送信は予測不可能である。アクセス制御システムにおいて、シリアル番号を示す固定部分は、コードホッピング部分により生成され得、共に、データ伝送インターフェースによって送信される送信値を形成し得る。

本発明の一実施形態において、符号化器学習能力が実行される。これは、ユーザが、ユーザによって選択可能である学習モード機能を有する、復号化器によって認識される符号化器を置換または追加することを可能にする。学習モード機能は、復号化器上でそれを起動することによって選択され得る。このことは、通常の符号化器を用い、復号化器を学習モードに設定するように出力機能をプログラムすることにより達成され得る。これはまた、マスタ符号化器またはトークンとしても知られている。このようなマスタ符号化器の使用は、より高いレベルのセキュリティが達成されることを可能にする。マスタトークンは、入力スイッチと組み合わせても用いられ得る。

本発明の別の実施形態において、符号化器が、外部入力値を符号化することが

可能である。この入力値は、符号化器によって内部的に符号化されるべき値に置き換わる。この場合、双方向通信構造が用いられる。この手順は、アクセス制御および認証を目的として、ｉｄｅｎｔｉｆｉｃａｔｉｏｎ ｆｒｉｅｎｄまたはｆｏｅ（ＩＦＦ）として知られる符号化器のオリジナリティを識別するために用いられ得る。符号化器は、アクセス制御システムの一部を形成するターミナルからの入力としてチャレンジ値を受け入れる。この入力値は、符号化機能およびキーを用いて符号化器によって符号化され、符号化値を形成する。次いで、符号化値は、アクセス制御ターミナルの一部である復号化器に伝送される。合法な符号化器が用いられている場合、符号化値は、復号化器によって演算された復号化値と一致し、復号化器は外部機能が動作することを可能にする。これが合法な符号化器でない場合、復号化値は、復号化器によって生成された値と一致せず、復号化器による必要な応答を阻止する。

符号化器は、アクセス制御システムにおけるトークンまたはトランスミッタ型装置内で用いられ得る。トランスミッタは概して、起動すると、符号化器出力からの情報を、無線（ｒｆ）、赤外線（ｉｒ）またはマイクロ波などの伝送媒体を介して受信システムに伝送する。トークンはさらに、トランスミッタ装置を指定し得るが、より概して述べると、情報の伝送が電気的接触および導電体によってなされる装置を含む。これらの物理的接触トークン（またはスマートカード）において、情報は読出しおよび書込み動作を介して双方向に伝送され得る。両方の場合において、本発明は、符号化または復号化キーを外部世界に露出する可能性なしに、符号化または復号化キーに関する情報を伝送することに向けられている。

一旦復号化器の学習モードが選択されると、新しい符号化器からのデータが捕獲されて、シリアル番号がまず用いられる。製造業者のマスタキーと捕獲された符号化器のシリアル番号とを利用して、新しい復号化器キーが、復号化器の一部を形成しているに違いないキー生成アルゴリズムによって誘導される。新しく誘導されたキーを用いて、既に捕獲された送信の変数（符号化された）部分を復号化する。この部分は、一旦復号化されると、正しいキーが生成されて用いられて

いることを検証するためにチェックされる。

別の実施形態において、さらなる送信が復号化される必要があり得る。この二重送信システムはさらに、その後、復号化されたカウンタ情報をチェックして、生成されたキーが有効であることを保証する。符号化器のシリアル番号が不揮発性メモリ内に格納され、不揮発性メモリ、誘導された復号化器キー、管理コード、

カウンタ、および他のユーザ情報と関連づけられる。従って、学習は、符号化器のシリアル番号が有効として受け入れられる前に検証され、その後符号化器が通常動作中に復号化器を起動するために用いられ得る。

通常動作において、符号化器は、例えばプッシュボタンスイッチ（単数または複数）を押すことにより又は他の何らかの適切なコマンド手段により電気的入力を介して起動される場合、アルゴリズムおよびキーで、カウンタ、ボタンおよび管理コード情報を符号化する。管理コード情報は通常、以下の群より選択された情報からなる：符号化器ステータス、コマンド、アイデンティティ、技術タイプ、時間、モード、完全性、およびユーザデータ。管理コード情報は、さらに時間情報をも含み得る。この時間情報は、符号化イベントが起こった時間を復号化器システムに伝送するため、または有効期間または満了日を復号化器システムに示すために用いられ得る。ユーザキーは、不揮発性メモリ内に格納されている情報の一部を形成するシリアル番号と関連づけられる。符号化されていないシリアル番号および符号化された情報は、外部データ伝送手段により伝送される。データ伝送は、符号化器による送信であり得る。あるいは、符号化器が、データを伝送するために特定のアプリケーションにおいて電気的に起動され得る。

復号化器は、送信を受信すると、符号化されていないシリアル番号と符号化された部分とを検出する。復号化器は、シリアル番号を、メモリ内に格納された、学習された符号化器のシリアル番号と比較する。匹敵が見い出されない場合、送信は拒否される。合致する値が見い出された場合、合致するシリアル番号に関連する、メモリ内に格納された復号化器キーを用いて、復号化アルゴリズムで、符号化された情報を復号化する。信号が受信され正しく復号化されたことを検証す

るために、送信の完全性がチェックされる。これが有効である場合、カウンタがチェックされる。有効である場合、復号化器カウンタ情報はアップデートされ、出力機能制御が起動される。カウンタが有効でない場合、送信は拒否される。

セキュリティシステムの利点は、送信が、ユーザからの介入なしに常に異なること、および学習プロセスが安全な様式で行われることである。学習復号化器は、アクセス可能で且つ使用可能でなければならない。製造業者のマスタキーに関する情報は復号化器内で使用可能でなければならない。

異なる実施形態において、さらに安全な学習プロセスが実行される。各符号化器について選択された独自のキー生成シードと共にアルゴリズムおよび製造業者のマスタキーを用いて、符号化器キーが生成される。キー生成シードおよびユーザキーは、符号化器のシリアル番号および管理コード情報と共に、各符号化器内にプログラムされる。キー生成アルゴリズムおよび製造業者のマスタキーは、いずれの符号化器内においても支配する必要がない。符号化器のシリアル番号とキー生成シードとの間に数学的リンクは存在する必要がなく、存在するべきではない。復号化器を新しい符号化器で学習する際、符号化器は学習モードに入れられ、キー生成シードおよびシリアル番号が復号化器に伝送される。復号化器は、製造業者のマスタキー、キー生成シード、およびキー生成アルゴリズムを用いて、この符号化器用のキーを生成する。キー生成シードが学習プロセスの間のみ送信されるため、無許可のアクセスは通常動作において不可能である。

正しいキーが生成され他の符号化器情報が格納されたことを検証するために、検証プロセスが開始される。完了すると、符号化器は有効符号化器となる。この検証プロセスはさらに、不良符号化器による送信、または製造業者の正しいマスタキーを有していない他の製造業者からの送信は学習され得ないことを保証する。

キー生成器シードを使用することにより、符号化器のシリアル番号が無断でスキャンされた場合にシステムのセキュリティが保護される。既知のシリアル番号を持てば、製造業者の装置および製造業者のマスターキーへのアクセスが得られるならば符号化器が偽造され得ることは、ほとんどありそうにないが、可能では

ある。しかし、キー生成器シードを使用する場合は、所有者の送信機またはさらにトークンへのアクセスを持たなければ、復号化器に格納されているキーを生成することはできない。

学習動作が成功裏に実行され、復号化器が通常動作モードに戻ると、符号化器を用いて、復号化器を通常の方法で起動させることができる。これは、シリアル番号が再び、学習されたシステムと比較されることを意味する。この反復プロセス中には特別なボーレート補償回路が用いられ、これにより、信頼性のあるコード反復を行うことができる。符号化器のシリアル番号に関連する格納されたキーは、送信を復号化するために使用される。受信され復号化された送信の完全性は、

符号化器から受信され復号化された管理コード情報を格納されている情報と比較することによって、有効性が検査される。同様のプロセスが、関連するカウンタ情報について実行される。成功の場合は、カウンタ情報がアップデートされ、所定の出力信号が選択され、この結果、正しい外部機能が起動される。

侵入者がキー情報を横取りしセキュリティシステムを危険にさらすのを防ぐために、キー情報は絶対に送信すべきではない。コードホッピングにより、侵入者が、コードを横取りまたは生成することによって、または無断のコードホッピング符号化器を初期化することによって、復号化器または復号化器の学習能力に無断のアクセスを行うことが不可能になる。

上述のシステムは、復号化器に格納されたキーを使用して受信を復号化する。学習システムの別の構成としては、復号化器のキー位置に、キー体ではなく、キー生成シードのみを格納することがある。復号化動作中、関連シード、シリアル番号および製造業者のマスターキーを選択することにより、正しいキーが生成される。これの利点は、キー生成シードはキーより必要な格納スペースが少なくてよいため、必要な非揮発性格納スペースが少なくてすむことである。正しいキーは必要なときにはいつでもＲＡＭ内に生成される。単一の復号化器に対して数個の符号化器が学習され得、またＲＡＭは繰り返し使用され得るため、これの実現は経済的である。

本発明は、製造業者が本発明の原理を利用することが可能な様々な異なる構成、例えば、乗物のセキュリティシステム、ドアまたはゲートのリモートコントロールセキュリティシステム、またはセキュリティ領域への職員のアクセスを制御するシステムにおいて使用され得る。また、例えば無線、赤外線または物理的な有線接続などの様々な異なるタイプの送信媒体が使用され得る。

本発明を、以下の添付図面を参照しての実施例によってさらに述べる。

図１は、本発明のアクセス制御システムの、符号化器およびデータ転送インターフェースと復号化器およびデータ転送インターフェースとを示す簡略ブロック図である。

図２は、図１の符号化器をより詳細に示すブロック図である。

図３は、図１の復号化器をより詳細に示すブロック図である。

図４ａおよび図４ｂは、本発明のシステムで具現化される学習アルゴリズムの動作のフローチャートである。

図５は、本発明の符号化器および復号化器で使用されるパラメータセットの格納フォーマットの図である。

本発明を以下に、先ず本発明の原理を示すために、図１を参照して一般的に述べ、次に、図２～図５Ｂを参照して、本発明の具体的な実施形態に関連してより詳細に述べる。

図１は、コードホッピング遠隔制御システムで使用される、符号化器１０とデータ転送インターフェース１１とを備えた送信機、および復号化器１２とデータ転送インターフェース１３とを備えた受信機の簡略ブロック図である。単に明瞭化のために、複雑な機能および多数の符号化器／復号化器の組み合わせは省略されている。

本発明は、主に、コードホッピングシステムでの学習の実現に関連する。学習は、標準固定コードシステムでは実現されているが、コードホッピングシステムでは固有の課題が存在する。符号化器によって符号化された情報は、ユーザキーへのアクセスを持たない場合は復号化することができず、この結果、符号化された情報を用いて、キーを復号化器に送信することができない。本発明はこの問題

を克服することを目指す。

符号化器は、ボタン符号化器１４と、カウンタ／格納およびエラー訂正部１６と、管理コード格納装置１７と、符号化アルゴリズムを有する非線形符号化器１８と、キー生成シードのための格納装置２０と、ユーザキーのための格納装置２２と、符号化器に関連するシリアル番号のための格納装置２４と、パルス幅変調コード生成器２６とを含む。

復号化器１２は、コントローラ３１と、フォーマット検出器３２と、復号化アルゴリズムを有する復号化器３４と、完全性検査部３５と、カウンタ値（同期化）検査ユニット３６と、出力管理機能３８と、製造業者のマスターキーのためのカウンタ／格納装置４０と、キー生成ユニット４２と、管理コードのための格納装置４３と、復号化器キーのための格納装置４４と、カウンタ情報のための格納およびエラー正部４６とを含む。

ボタン符号化器１４は、手動で作動可能の複数のボタン４８に応答する。ボタンが作動されると、符号化器１０が全体として作動される。符号化器は、以下の記述により明らかとなり得るように、複数のモードのうちの任意のモードで機能し得る。符号化器の動作モードは、作動されるボタンによってまたはボタンの組み合わせによって決定される。符号化器の機能はコントローラ４９によって制御される。

符号化器制御のコントローラ部４９は符号化器の動作を制御する。制御部４９は符号化器の各部に接続され、各部の動作状態を感知して動作制御信号を各部に供給して、全体として符号化器の動作および機能を制御する。符号化器コマンドが外部ボタンから受け取られ、符号化器の残りの部分への動作制御信号を初期化するために用いられる。制御信号は、符号化器モード変更、送信情報の選択、および必要に応じて異なる部分すべての起動よりなる。

復号化器のコントローラ３１は、符号化器制御部４９が符号化器を制御するのと同様の方法で復号化器を制御する。制御部３１は復号化器の各部に接続される。制御部は復号化器の各部の動作状態を感知し各部に動作制御信号を供給して、フォーマット検出器から受け取られる復号化器コマンドおよびモード選択入力信

号から、全体としてのデコーダの動作および機能を制御する。制御信号は、復号化器モード変更、キー生成の選択、キーおよびシリアル番号などの情報の格納、完全性検査、同期化およびカウンタ値格納装置、および出力信号よりなり得る。

コントローラ４９は２つのモードのいずれか、すなわち、学習モードまたは通常動作符号化モードで機能し得る。各モードは、上述のように、ボタン４８の適切な選択によって、またはアプリケーションでの符号化器の構成に特有な任意の他の適切な方法によって選択され得る。ボタン符号化部１４によってコマンドが入力されると、制御部４９によって制御信号が発行される。通常動作モードでは、制御信号は、カウンタ／格納およびエラー訂正部１６、管理コード格納装置１７、非線形符号化器１９、キー格納装置２２、シリアル番号格納装置２４、およびＰＷＭコード生成器２６を動作させるために発行され、各特定部の適切な出力を選択および起動させる。これにより、符号化器が、以下により具体的に記述するように機能することが確実となる。

符号化器が学習モードで使用される場合は、制御部４９は、シード格納装置２０、シリアル番号格納装置２４、およびＰＷＭコード生成器２６に対して制御信号を発行し、各特定部の適切な出力を選択および起動させる。これにより、符号化器が、以下により具体的に記述するように機能することが確実となる。

復号化器のコントローラ３１は、２つのモード、すなわち、学習モードおよび通常動作符号化モードのうちのいずれかで機能し得る。モードは、適切な内部または外部回路によって選択され得る。内部回路は、以下に示すような通常の検出および復号化動作によって起動され得、復号化器を学習モードにする。プッシュボタン１１０または他の切り替え手段などの外部回路も同様に使用され得る。好ましくは、１つの実施形態によれば、物理的に符号化器および復号化器から離れているかまたはこれらから外されている復号化器学習モード起動手段を含むことが、より簡便且つ安価であることが発見されている。例えば、１つの実施形態によれば、本発明の符号化器／復号化器システムがガレージドア開閉システムで利用される場合、復号化器／受信機学習モード起動手段は、好ましくは、物理的に受信機（または送信機／符号化器）上に位置するのではなく、受信機／復号化器

と電気接続しているガレージの壁に位置する。好ましくは、学習モード起動手段は、送信機／符号化器をガレージドアの開閉に利用しないときに、ガレージドアの開閉に利用される壁コンソールスイッチの一部である。好ましくは、壁コンソールスイッチは、例えばボタンを長い期間（例えば５秒間）押し続けることによって、スイッチが起動されると、受信機／復号化器が学習モードに設定されるように構成される。好ましくは、壁コンソールスイッチまたはボタンが短い期間しか起動または押し下げられないときは、ガレージドアの開閉がそれぞれ行われる。

通常の動作モードでは、一旦、復号化器が、フォーマット検出器３２を用いて、受信信号を検出すると、コントローラ３１は、制御信号を決定し、復号化器を動作させる。制御信号は、キー生成アルゴリズム／制御４２、キー格納装置４４、復号化器３４、管理格納装置４３、完全性検査３５、カウンタ／格納装置およびエラー訂正部４６、カウンタ値検査３６、および出力管理３８に発行され、各々の特定の部分の適切な出力を選択して起動させる。これは、符号化器が、以下により具体的に説明されるように機能することを保証する。

復号化器が学習モードで使用されると、コントローラ３１は、キー生成アルゴリズム／制御４２、キー格納装置４４、復号化器３４、管理格納装置４３、完全性検査３５、カウンタ／格納装置およびエラー訂正部４６、出力管理３８、および学習制御１００に、コマンドを発行する。これは、復号化器が、適切な情報を格納し、且つ、以下により具体的に説明されるように機能することを保証する。

通常動作モードでは、カウンタ／格納装置およびエラー訂正部１６は、符号化器１０が使用されるたびに起動される。従って、そのカウントは、符号化器が使用された回数を示す。カウンタ値は、不揮発性メモリに格納される。メモリは、符号化器に電力が供給されたときにのみ動作する。カウンタ値が変化し、それと同時に電力が遮断されると、不正（spurious）値が格納され得る。この理由のため、エラー訂正機能は、カウンタ／格納装置およびエラー訂正部１６に含まれる。カウンタ情報は、格納装置２２中のユーザキーを用いて、非線形符号化器１８で符号化される。従って、符号化器１８の出力は、生成器２６において、格納装

置２４からのシリアル番号と組み合わせられる変数情報を含む。上述のように、シリアル番号は、符号化器と関連する。生成器２６の出力は、データ転送インターフェース１１に与えられ、データ転送インターフェース１３および復号化器１２に送信される。シリアル番号はまた、符号化器ユニットを同定するための固有のユニット番号の一部分を形成し得る。

尚、符号化器および復号化器は、例えば配線などによって直接接続されてもよく、または、符号化器および復号化器は、互いに遠隔にあってもよく、情報の送信は、無線信号によって行われ得、光学的には、赤外周波数または他の任意の適切な方法で行われ得る。

データ転送インターフェース１３を用いて復号化器１２により受信される信号は、論理信号に変換され、この論理信号は次に、フォーマット検出器３２によって、復号化器３４に与えられる番号に変換される。検出器は、パルス幅変調コード検出器であり得る。復号化器３４の復号化アルゴリズムは、カウンタおよび管理コード情報を生じる番号の変数部分を復号化し、そのカウンタおよび管理コード情報の完全性は、格納装置４５の中にある管理コード情報を用いて、部分３５によって検査され、復号化動作の有効性を確認する。復号化動作が有効であれば、

ユニット３６は、復号化されたカウンタ情報を、格納装置４６に保持されたカウンタ情報と比較し、復号化された番号が有効であり且つ以前に使用されていないと判定する。受信が有効であれば、出力管理機能３８によって、関連する出力が起動される。

学習を実現するために、ユーザは、復号化器１２を学習モードにする。好ましくは、１つの実施形態によれば、これは、復号化器から物理的に分離されたまたは遠隔にある学習モード起動手段を起動させることによって達成される。符号化器１０はまた、適切なボタン４８の起動によって、効果的に学習モードにされる。この場合、格納装置２０に保持されるキー生成シードは、格納装置２４中のシリアル番号とともに、生成器２６に与えられる。尚、キー生成シードは、学習動作中にのみ使用される。復号化器の動作全体は、コントローラ３１によって制御

される。

従って、データ転送インターフェース１１は、キー生成シードおよびシリアル番号についての情報を、復号化器１２に送信する。データ転送インターフェース１３は、この情報を受け取り、この情報はその後、検出器３２によって検出され、キー生成ユニット４２に送られる。このユニットは、入力されるキー生成シードと、格納装置４０に保持される製造者のマスタキーとに基づいて、復号化器キーを計算する。この新しく生成された復号化器キーは、場所４４に格納され、未来の任意の符号化動作のために使用され得、復号化器３４の復号化アルゴリズムに作用する。

安全な学習動作の間にキー生成ユニット４２において使用されるキー生成アルゴリズムは通常、非線形アルゴリズムである。このアルゴリズムは、製造者のマスタキー４０（図示せず）およびキー生成情報を、入力として受け入れる。キー生成情報は、符号化器シリアル番号２４からなるか、シード２０からなるか、またはその両方からなり得る。この情報は、学習動作において符号化器から復号化器に転送される。

復号化器１２は、キー生成アルゴリズムを用いて、通常のコードホッピング送信を復号化するために使用されるキー４４を生成する。この機構のセキュリティは、送信されたシードと復号化キーとの間の関係が知られておらず、送信の任意の種類の干渉を無駄にすることに関係する。非線形キー生成機能はまた、キーとキー生成情報との間の任意の関係の確立を不可能にし、詐欺師が、合法でない符号化器をコピーする可能性をなくす。符号化器１０のキー２２、シリアル番号２４、およびランダムに生成されたシード２０は、製造プロセスの間にロードされる。製造者は、シード、シリアル番号、製造者のマスタキー、およびキー生成アルゴリズムを用いて、キーを生成する。キー生成アルゴリズムは、公には知られないようにされる。シードがランダムな数であるため、同じキーを有する２つの符号化器を製造する可能性は、非常に少ない。このプロセスでシリアル番号も使用されることを考慮すると、その可能性は、極めて低い。

学習プロセスの確認は、以下のように行われる。ユーザは、符号化器１０の通

常動作のための適切なボタン４８を押し、それにより、非線形符号化器１８によって生成される変数コード、および格納装置２４に保持されるシリアル番号の送信を引き起こす。格納装置４４中の新しく生成された復号化器キーは、復号化器３４の復号化アルゴリズムにおいて、入力されるコードを復号化するために使用される。これにより生成される管理コード情報は、この管理コード情報を、格納装置４３中の管理コードと比較することによって、復号化動作の有効性を確認するために使用される。入力されるカウンタ情報は、関連する格納場所４６に格納される。エラー訂正機能はユニット４６に含まれ、電源異常の間に不正データが格納されると、復号化器への電源が回復されるとすぐに、正しいデータが回復され得ることを保証する。

その後、ユーザは、符号化器１０を再び起動させる。その結果得られた変数コードおよびシリアル番号は、もう一度、データ転送インターフェース１３によって受け取られる。変数コードは、新しく生成された符号化器キーを用いて、復号化器３４の復号化アルゴリズムによって復号化される。この送信から得られるカウンタ情報は、格納場所４６に保持されるカウンタ情報に対して検査される。この比較により、２つの変数コード送信が成功であったことが示されると、学習プロセスが有効であったと仮定され、復号化器は、学習モードから出される。この時点で、システムは、通常動作のために使用され得る。

格納装置２０中のキー生成シードと、格納装置２２に保持されるユーザキーとの間には、特別な関係がある。この関係は、格納装置４０に保持される製造者のマスタキーに依存する。しかし、製造者のマスタキーは、符号化器にはプログラムされず、その代わりに、対応するキー生成シードおよびユーザキーをそれぞれの符号化器にプログラムする生産ラインプログラミングユニットにおいて使用される。一方、製造者のマスタキーは、各復号化器にプログラムされ、学習中に、説明された態様で使用され、受け取られたキー生成シードから、正しい復号化器キーを計算する。この復号化器キーはその後、格納場所４４に保持される。

学習プロセスの変形では、格納装置２４に保持されるシリアル番号は、キー生成ユニット４２によって使用され、復号化器キーを生成する。この場合、符号化

器が、キー生成シードを転送する能力を有している必要はない。さらに、キー生成シードとユーザキーとの間にではなく、シリアル番号とユーザキーとの間に特別な関係がある。

シリアル番号は、各送信中に存在する。従って、そこから送信が起こる符号化器は、外部者が、送信に含まれる情報へのアクセスを獲得することができなくても同定され得る。シリアル番号は、1つのシステムにおいて幾つかの符号化器を同定するために使用され得、1つの複号化器システムにおいて、幾つかの異なる符号化器を収容することを可能にする。

添付の図面の図2および図5に基づく以下の説明は、図1とともに説明してきた一般原理を実施する、本発明の制御システムの実際の形態を参照して行われる。適用できる場合には、図1で使用される参照番号と同様の参照番号が、図2から図5において、同様の構成要素を示すために使用される。

図2は、符号化器10と、ボタン48と、コントローラ49と、電源50と、データ転送インターフェース11とを含むコードホッピングリモートコントロール送信機の実装を図示する。これらは全て、綴輪に取り付けられユーザが簡便に送信機を携帯することができる保護性ハウジングに収容され得る。ボタン48は押しボタンスイッチであり得、セキュリティシステムの様々な機能をリモートコントロールによって起動し、あるいは、電池であり得る電源50から送信機全体に電力を供給する。

電源50、ボタンスイッチ48およびデータ転送インターフェース11以外のブロック図に示される要素の全ては、単一の集積回路によって実装され得る。特定用途集積回路は、リバースエンジニアリングをなるべく難しくするためには好適な実装例である。リバースエンジニアリングは、アルゴリズムおよび格納情報への完全なアクセスがこのプロセスによって提供されるので、セキュリティシステム内でのセキュリティ上に危険性を与える。

符号化器10は、押されたボタン48に関する情報を符号化する手段14（ボタン符号化器）を含み、符号化された情報52を出力する。この符号化された情報52は、コントローラ49および他の部分を用いて符号化器の動作を制御する

ために用いられ、「機能要求」(function request)として符号化され得、復号化器１２によって起動される機能を決定する。制御機能は、シリアルコード生成器２６の動作のモードを選択し、エミュレートされるバーチャル符号化器を選択する。（用語「バーチャル符号化器」の意味は、以下の説明から明らかになる。）機能要求は、復号化器上のいくつかの出力のうちの１つを起動し得る。異なる復号化器出力を用いてイモビライザ(immobilizer)を解除したり、アラームをセットしたり、アラームを解除したり、車の電動式ウィンドを操作し得る、車のセキュリティシステムが典型的な用途の１つであろう。

ボタン符号化器１４の実施例は、ボタン量bが符号化器を起動するのに用いられた場合、ボタン符号化機能が値bを符号化器の内部回路に伝えられる区別可能な値に符号化する。２つのボタンを同時に押すことは、例えば、ボタン符号化器１５による区別可能な値の生成を開始し得、区別可能な値は、符号化器関連情報を転送するように符号化器を起動する。同じ２つのボタンのうちのどちらか１つが個別に用いられたとき、全く異なる値がボタン符号化１４によって生成され、その結果、異なる情報を選択し、転送する。これは、ボタン量bのみを用いて、２のb乗の異なる機能が区別および選択できることを意味する。ボタン符号化１５は、また、符号化機能が所定値を出力するようにプログラムすることによって符号化器を学習モードに設定するために用いられ得る。この値は、任意の１つまたは組合せのボタンが押されたときに与えられ得る。

不揮発性メモリ５４の１セクションは、複数のパラメータセット５６Ａ～５６Ｎを格納するために用いられる。各パラメータセットは、図１の格納装置２０に

保持されるシードに対応する固定キー生成シード６０、図１の格納装置２４に保持されるシリアル番号に対応するシリアル番号６２、格納位置２２に保持されるユーザキーに対応する符号化またはユーザ２０のキー64、カウンタ／格納およびエラー訂正１６に保持されるカウンタ情報を含むカウンタおよびエラー訂正情報６６、ならびに格納装置１７に保持されるコードに対応する管理コード６８からなる。

上記のように、いくつかのパラメータセット５６を格納装置が提供される。各

パラメータセットは、本明細書中では「バーチャル符号化器」と呼ばれるものの１つに関連づけられる。なぜなら、符号化器がボタン４８のうちのどれが押されるかによって複数の異なるバーチャル符号化器の任意の１つとして機能し得るからである。

カウンタ／格納およびエラー訂正１６は、符号化器が作動されるたびにアップデートされる。しかし、いくつかのパラメータセットが用いられる場合、対応するバーチャル符号化器が用いられるたびに特定のパラメータセットのカウンタ情報のみがアップデートされる。

特定の符号化器は、様々な機能要求と共に単一の格納されたパラメータセット５６または、同様または異なる機能要求を有する異なるパラメータセットのどちらかを用いることが可能である。典型的に、いくつかの異なる復号化器がアクセスされる場合は異なるパラメータセットが用いられる。いくつかの機能１５は、各復号化器上でアクセス可能であり得る。単一の符号化器は、異なるパラメータセットを用いて全ての復号化器にアクセスするように構成され得、異なる機能要求をパラメータセットのそれぞれと組み合わすことが可能になり得る。

シリアル番号６２は、特定のバーチャル符号化器に対して固有であり、その特定のバーチャル符号化器からの発生物と共に符号化される。符号化またはユーザキー６４は、特定のバーチャル符号化器に固有の数であり、オリジナルの符号化された情報が外部者から読み出されない方法で送信を符号化するために用いられる。管理コード６８は、特定のバーチャル符号化器のステータスについての情報からなり、復号化器内の復号化動作の完全性を検査する所定の値を有するセクションを含み得る。カウンタおよびエラー訂正情報６６は、１６ビットカウンタの

カウントであり、符号化器と復号化器との間の同期および、格納動作中に偽エラーが生じた場合に訂正されたエラーのトラックを維持するために用いられる。カウンタは、バーチャル符号化器が動作するたびに変更される。キー生成シード６０は、図１を参照にして記述したように、符号化キー６４との特定の関係を生じさせる数である。キーは読み出し禁止されているが、シード６０は必ずしもアクセス不可能ではない。しかし、この２つの関係は十分に不明瞭であり、外部者は

シードの値からキーを推測することはできない。

不揮発性メモリ５４は読み出し禁止であり、外部からの符号化キー６４の精査を防止する。キーまたはシリアル番号６２、シード６０および格納装置４０内の製造業者のマスタキーへのアクセスは、外部者が同一のキーを用いて同様の符号化器をプログラムし、システムにアクセスすることを可能にし得る。

符号化器は、ユーザキー６４を用いて入力ストリングを符号化する非線形符号化器１８を含む。コンピュータ技術の現状を考慮すると、キーの長さは暗号解析(analytical attack)に対して適度な耐性を確保するように十分な長さにするべきである。６４ビットのキーの長さは、セキュリティおよびアクセス制御システムのために妥当であると考えられる。より長いキーを用いるとコストに関して不利になり、より短いキーは、低下したセキュリティレベルを提供する。非線形符号化アルゴリズムの出力ストリング７０の長さは、符号化器によって符号化されるビット数を決定する。３２ビット出力ストリングは、セキュリティと典型的なリモートコントロール送信速度での応答時間との間に良好なバランスを提供する。符号化アルゴリズムへの入力ストリングは３２ビットであり、起動される符号化器に特定のボタン符号化器１４（４ビット）からの機能情報５２、カウンタ情報６６（１６ビット）、および管理コード６８（１２ビット）を含む。管理コードは低バッテリ電圧インジケータおよびモード選択を含むシステムステータス情報を含み得る。

シリアルコード生成器２６は、発せられるコードを組み立てるために用いられる。コードは、非線形符号化器１８によって生成される３２ビットの符号化されたストリング７０と符号化器のシリアル番号６２との組合せ、または、固定キー生成シード６０とシリアル番号６２との組合せからなり得る。コード生成器２６は、また、データ転送インターフェース１１による送信に必要な変調スキームを実現する。この場合の変調スキームはパルス幅変調(ＰＷＭ)である。

シリアルコード生成器２６の出力７２は、電磁気または他の手段を用いてインターフェース１１によって発せられる。データ転送インターフェース２８は、リモート操作が必要でない場合に直接接続によって置換され得る。

符号化器は、選択されたオプションおよび符号化器内にある条件に依存して特定のメモリブロック内の管理コード６８の部分、例えば、ステータス情報、を変更し得るステータスモニタ７４を含む。これらの変更は、復号化器によって検出され得、目前の符号化器問題、例えば、バッテリ切れのフィードバックを提供する。監視されているステータス局面は、ユニット７６を介して選択される。

オプション７６は不揮発性メモリ内の符号化器にプログラムされ得、ステータスモニタ７４によって異なる符号化器ステータスを選択する。特定の所定のオプションは、例えばバッテリ低電圧を表示し得る。ｓａｍ値(sam value)は、送信中のバッテリ蓄電池低電圧の表示を感知して、それをユーザに表示するように復号化器にプログラムされる。これにより、符号化器が起動されたときプログラムされたオプション７６は起動され、これにより、選択されたステータスモニタ７４も起動される。所定値は情報を符号化して転送する前に管理コード６８の一部分に代用される。このオプションは、選択されて転送されたとき復号化の後復号化器によって感知され、これによりプログラムされた作動が取られ得る。

図３は、学習コードホッピングアクセス制御復号化器の実装を図示する。

データ転送インターフェース１３は、データ転送インターフェース１１からの信号の送信に用いられる電磁気信号または他の信号を、シリアルコード生成器２６によって実現された変調スキームによって依然として変調されているベースバンド論理信号７８へと変換する。

復号化器は、符号化器と復号化器との間の異なるタイミングによる送信長の違いを補償する手段を有する検出器３２を含む。

検出器３２は、３２ビット変数８０を信号７８から抽出し、これを不揮発性メモリ８４に格納される６４ビット復号化器キー８２を用いて変数を復号化する復号化アルゴリズム３４に適用する。有効な復号化プロセスが行われた場合、結果

として生じる３２ビットコード８６は、符号化する前に符号化器１０内の符号化器１８の非線形符号化アルゴリズムに挿入される情報を含む。

復号化器は、復号化プロセスの有効性を確認する完全性検査ユニット３５を含む。有効な復号化については、図１の格納装置４３中に保持されたコード対応す

る格納された管理コード９０と復号化された３２ビットワード８６の対応部分との間に所定の関係がある。

復号化器キー８２は、図１の復号化器１２の格納位置４４に保持される復号化器キーに対応する。

同期検査ユニット３６は、完全性検査ユニット３５によって生成された入来カウンタ情報９２と関連する符号化器について格納されたカウンタ情報９４とを比較することによって、送信の有効性を確認する。カウンタ情報９４は、図１の復号化器１２の格納位置４６に保持される情報に対応し、停電中に偽エラーが格納されたときにカウンタ値を訂正することを確実にするエラー訂正機能を含む。

出力管理ユニット３８は、システム中の他の装置の起動、またはこのような装置との通信を管理する。ユニット３８は、いくつかある機能のうちのどの機能が所望であるか、符号化器１０が符号化を終止したかどうか、特別なオプションが要求されたかどうか、の表示を提供する。受信信号が発せられる符号化器のアイデンティティの表示も利用可能にされ得る。ユニット３８は、不揮発性メモリ８４中の格納スペースを使用し、オプション制御ユニット９６によって決定されるオプションを管理する。このオプションは、ユニットによって生成された出力信号９８が呈示するフォーマットに影響を与えるか、または、特定システム特徴をイネーブルまたはディセーブルにし得る。

学習制御ユニット１００は、検出器３２、復号化器の復号化アルゴリズム３４、完全性検査ユニット３５、同期検査ユニット３６、およびキーアドレス管理ユニット１０２とに適切な命令を伝える学習プロセスを管理する。ユニット１００は、復号化器の外から学習モードにすることができるか、または、特別な出力組合せが、管理制御ユニット３８から学習制御ユニット１００へと関連する信号を伝えることよって復号化器を学習モードにするために用いられ得る。最も好適であるのは、例えば、復号化器から物理的に離れるまたは分離したスイッチまたは回路

などの学習モード起動手段によって、復号化器を学習モードに設定するシステムである。好ましくは、学習モード起動手段は、符号化器からも物理的に離れるま

たは分離している。典型的には、単一のメモリブロックがこの目的のために確保される。学習制御１００を含む復号化器は、コントローラ３１によって制御される。

マスタ符号化器と呼ばれる指定された符号化器のパラメータセット５６は、この確保されたメモリブロック内に格納される。マスタ符号化器が起動されたとき、出力機能制御ユニット３８はユニット１００に制御信号を送出し、復号化器１２を学習モードにする。

不揮発性メモリ８４は、符号化器内のパラメータセット５６Ａ～５６Ｎに対応する複数のパラメータセット１０２Ａ～１０２Ｎの格納装置を提供する。各パラメータセットは、対応する符号化器のシリアル番号６２に対応するシリアル番号１０４と、関連復号化器キー８２と、管理コード９０と、カウンタ情報９４とを含む。図１の格納位置４０に保持される情報に対応する製造業者のマスタキー１０６もまた、学習動作中に用いられるためにメモリ８４内に格納される。

キーアドレス管理ユニット１０２は、不揮発性メモリ８４への／からの情報の経路を管理する。キーアドレス管理ユニットは、ハードウェア、ソフトウェア、またはそれらの組合せにおいて実装され得る。このユニットは、用いられるメモリバンクを選択し、各メモリバンクは、単一のパラメータセットを格納することができる。ポインタも、メモリセグメント１０８内に維持され、学習動作に用いられる次のメモリバンクを表示する。

学習動作中、キー生成ユニット４２は新しい符号化器用の復号化キー８２を生成し、それをそれぞれのパラメータセット１０２のための関連するメモリ位置に転送する。コードホッピングアルゴリズムと複雑さが同様な非線形符号化アルゴリズムが、キー生成シードと符号化または復号化キー８２との関係ができるだけ不明瞭になることを確実にするために用いられる。

図５は符号化器パラメータセット５６と復号化器パラメータセット１０２との表示を含み、各パラメータセットの内容の概略を含む。

ユーザが符号化器１０を起動するためにボタン４８を押したとき、ボタン符号化ユニット１４が、どちらのボタンまたはボタンの組合せが押されたかを判定し

、制御信号の組合せと共に４ビット機能コード５２を生成する。制御信号は、どちらのメモリブロックから関連するパラメータセットが取られるか判定し、送信がホッピングコードからなるべきかまたは固定コードからなるべきかを判定する。

ボタン４８は、符号化器を電気的に命令することができるシステムによって置換され得る。命令は、例えば、コンピュータまたは他の機器によって、特別な命令インターフェースを用いて生成され得る。符号化器の電源も、また、命令インターフェースによって供給され得る。

別の応用において、符号化器と復号化器との組合せが、認証およびアクセス制御目的のために用いられ得る。符号化器は、トークンまたはスマートカードに収容され得、人が、例えば、携帯および使用して警備領域にアクセスすることができる。通信は、電気的インターフェースで起こる。この場合、符号化器と復号化器との間で情報を通信するために、双方向通信が用いられる。符号化器のシリアル番号６２は、復号化器に転送され、復号化プロセスで用いられるキー８２を確立する。復号化器によって、チャレンジ(challenge)として知られる値が符号化器への入力値として与えられる。符号化器は、チャレンジ値を符号化し、符号化した値を復号化器へ戻す。そして、復号化器が符号化された値を復号化し、それをチャレンジ値と比較して符号化器の確実性を確立し、それに従って出力を起動する。この技術は、一般的にＩＦＦ（敵味方識別(identification freind or foe)）として公知である。この応用において、符号化器のシード６０は、学習モードの復号化器に転送され得る。キー８２は、この説明中に記載したように復号化器内で生成および格納され得る。

１つの符号化器に対して１つ以上パラメータセットを利用できる能力は、単一の動作周波数が共有されていても、符号化器が１つ以上の復号化器に干渉なしにアドレスすることを可能にする。符号化器は、各々独立の動作をすることが可能な、いくつかの独立符号化器のうちから選択された１つであるように思われるので、「バーチャル符号化器」と呼ばれる。明らかに、符号化器は、同時に動作することはできない。ホッピングコード動作に対して、符号化器１８の非線形符号化アルゴリズムは、それぞれの符号化キー６４を用いてカウンタ情報６６と管理

コード６８とを４ビット機能コード５２と共に符号化する。３２ビット出力コード７０が、シリアルコード生成器２６に与えられる。カウンタ情報６６は、それぞれのバーチャル符号化器に対して送信が行われるたびに変更される。シリアルコード生成器２６は、符号化された部分に関連する符号化器のシリアル番号６２を付加し、これによって単一の出力コード７２を形成する。出力コード７２は、データ転送インターフェース１１の入力に（この実施例では）ＰＷＭシリアル形式で与えられる。

固定コード動作に対して、キー生成シード６０がシリアルコード生成器２６に直接与えられる。シリアルコード生成器２６は、コードをシリアル番号６２と共にＰＷＭシリアル形式でデータ転送インターフェース１１に与える。

両動作モードにおいて、データ転送インターフェース１１は電磁気または他の手段を用いてシリアルコード生成器から情報を送信する。

データ転送インターフェース１３によって受信された信号は、やはりＰＷＭ形式の論理信号７８に変換される。フォーマット検出器３２は、論理信号７８を監視し、明らかに有効な信号の最初の部分が観測されたとき、検出器は入来信号に対してそれ自身を較正し、名目のタイミングからの異常性を補償する。入来信号の残部は受信され、本実施例では６４ビット２進数に変換される。

検出器出力の最初の３２ビット、すなわちホッピングコードは、８０とし、復号化器３４の復号化アルゴリズムに示される。最後の３２ビット、すなわちシリアル番号は、キーアドレス管理ユニット１０２に与えられる。このユニットは、受信されたシリアル番号と格納されたシリアル番号１０４をマッチングが見出されるまで比較することによって、使用されるメモリブロックを決定する。復号化アルゴリズム３４は、正しいメモリブロック、すなわちそれぞれのパラメータセットからの復号化器キー８２を用いてホッピングコード８０を復号化する。３２ビット出力８６は、完全性検査ユニット３５に与えられる。この３２ビットストリングは、オリジナル４ビット機能コード５２、１６ビットカウンタ情報６６、および１２ビット管理コード６８を含む。完全性検査ユニット３５は復号化ワード８６中の復号化管理コード６８と格納されたバージョン９０との間の所定の関係を検査する。ある定義された関係が存在する場合、その復号化は有効であった

ものとする。

復号化されたカウンタ６６を、各パラメータセット中に保持されている格納されたカウンタ９４と比較する。同期により送信が有効であることが証明されると、格納された値９４がアップデートされ、出力制御機能ユニット３８に然るべく通知される。

ユニット３８は、復号化された機能情報９８を出力する。ユニットは、この情報を、外部コントローラによる使用のためにシリアルフォーマットで利用可能にしてもよく、あるいは、複数の異なる条件のうちのいずれかを示す別々の出力を有してもよい。管理コード、有効信号インジケータ、および第２の機能モードの一部として含まれ得る、復号中の符号化器のアイデンティティはすべて、有用な出力情報９８の例である。

学習動作は、ユーザがシステムに新しい符号化器を追加したいときに起こる。学習制御ユニット１００は次に、例えばスイッチ１１０を起動することにより、学習モードに入ることを促す入力信号を受信する。好ましくは、前述のように、スイッチ１１０は復号化器および符号化器から物理的に離されてあるいは隔たれている。信号は、前述のように、例えばスイッチによって生成される外部からの命令の形であるか、あるいは有効なコードの受信後に出力機能制御ユニット４８から出されてもよい。

そしてユーザは、特定の学習ハードウェア構成を用いて、符号化器１０を固定コード符号化器として起動する。キー生成シード６０を送信の変数コード部に代用し、シリアル番号６２を符号化コードの残りとして維持する。

結果として得られる、データ転送インターフェース１１から発せられる信号は、データ転送インターフェース１３によって受信される。フォーマット検出器３２は、受信された送信７８の全体を、キーアドレス管理ユニット１０２に渡す。従って、ユニット１０２に与えられる信号は、６４ビットのストリングである。ユニット１０２は、学習モードにおけるその通常機能から逸脱し、シリアル番号、キー生成シードおよび製造者のマスタキー１０６から、復号化キー８２を生成する。このキーが、この目的専用に用いられるメモリブロック１０８中に保持されたポインタの値に依存して、メモリブロックのうちの１つに書き込まれる。受

信

されたシリアル番号１０４は、各パラメータセットに関連付けられた対応するメモリブロック中に格納される。次の学習ポインタは、様々な異なるスキームに基づいて管理され得る。なかでもオプションとして、ポインタを利用可能なメモリ位置中をサイクルさせ、ユーザが外部からポインタを設定することを可能にすることが、包含される。

セキュリティ的な観点から、ユニット４２によって行われる種類のキー生成アルゴリズムは、アプリケーション専用集積回路においてのみ実現されるべきである。なぜなら、一般論理デバイス（例えばマイクロプロセッサなど）はリバースエンジニアリングが容易であることにより、アルゴリズムを大衆の精査に曝すからである。

そしてユーザは、符号化器をコードホッピングモードで２回起動する。１回目の送信において、６４ビットのコードがデータ転送インターフェース１３によって受信され、検出器３２によって検出される。復号化器３４の復号化アルゴリズムは、新しく生成された復号化器キー８２を用いて３２ビット可変長コード８０を復号化し、復号化された管理コード９０を正しい位置に格納する。復号化されたカウンタ情報９４もまた正しい位置に格納される。

第２の送信において、受信された信号は検出器３２によって検出され、シリアル番号がキーアドレス管理ユニット１０２に渡され、新しく格納されたシリアル番号１０４と比較される。さらに、３２ビット可変長コード８０が復号化アルゴリズム３４によって復号化される。完全性検査ユニット３５が、復号化された管理コードを格納されたバージョン９０に対して検査し、同期検査ユニット３６が、復号化されたカウンタ情報を格納されたバージョン９４に対して検査する。もしこれらの検査のいずれかが不成功であると、学習動作は拒絶される。もしこれらが全て成功すると、格納位置１０８中の次の学習ポインタが変更されることにより、次のメモリブロックが学習に利用可能であることを示す。

学習プロセスはまた、特定の符号化器に用いられる特定の出力の組み合わせを学習するためのルーチンを含み得る。例えば、特定のユーザは、特定のシステム

において特別の優先順位を必要とし得るため、そのようなルーチンにおいてこの優先順位を割り当てることができる。

学習動作全体が首尾よく完結すると、ユーザは、符号化器をもう一度起動することにより、符号化器が正しく動作していることを確認する。

上述のシステムは、復号化器において格納されたキー８２を用いることにより、入来する送信を復号化する。学習システムの別の構成として、キー全体の代わりに、キー生成シードのみをキー８２に割り当てられた位置に格納する。復号化動作において、正しいキーが、関連付けられたキー生成シードおよび製造者のマスタキー１０６から生成される。この利点は、キー生成シードは典型的にはキーよりも少ない格納スペースを必要とするため、必要とする不揮発性格納スペースが少なくなることである。正しいキーは、必要なときいつでもRAM内において生成される。

図４ａおよび４ｂは、復号化器において実現される学習アルゴリズムのフローチャートである。図４ａを参照して、前述のように学習モードが確立されると、キー生成シード（段階１５０）およびホッピングコード（段階１５２）が、復号化器によって受信される。段階１５４においてリレーショナルカウンタ（キー生成ユニット４２中の）が初期化され、ゼロにセットされる。リレーショナルカウンタを用いて、キー生成シードと符号化器シリアル番号と符号化器用のキーとの間、あるいは符号化器シリアル番号と符号化器用のキーとの間において、１つ以上の関係を可能にする。

段階１５６においてリレーショナルカウンタ１５４を用いて、少なくとも製造者のマスタキー１０６およびキー生成シードを入力として用いる非線形アルゴリズムであるキー生成アルゴリズム用に、変更された(modified)シードを作成する。キーが生成された後（段階１５８）、管理コードを復号化して格納し得る（段階１６２）。段階１６４において復号化動作の完全性を検査することにより、復号化動作が有効であるか否かを判定する。有効であれば、フローは段階１７０に進む。有効でなければ、動作が続けられるべきか否かを段階１６６において判定する。動作が続けられるべきならば、リレーショナルカウンタ１５４をインクリ

メントする（段階１６８）ことにより、有効かもしれない新しい関係を確立する。

キー生成シードとシリアル番号との間の全ての有効な関係が用いられても有効な関係（段階１６６）が見つからなかった場合、段階１７２において学習プロセスは終了する。

学習中に偶発的に無効な符号化器を容認してしまう確率は、符号化された管理コード内の所定のビットの数に関係する。説明している実施態様においては１２ビットより多くを利用することは可能でないため、最高の完全性は、４０００中１程度である。このレベルは、セキュリティシステムには不十分であると考えられる。わかっている管理コードの成分の長さを増大するか、学習中の符号化器からの第２の送信に基づく検査アルゴリズムを実現することにより（図４ｂの段階１７６）、完全性を改善することができる。より長いコード長を用いると、実現コストが高くなり、応答時間が長くなるという欠点を有する。第２の送信を用いることにより、システムコストまたは応答時間に影響することなく、完全性検査の確実さが何桁も増加する。

図４ｂを参照して説明されるフローチャートの第２の部分が、この技術を実現する。復号化機能が行われて有効であると見なされた場合（段階１７０）、復号化されたカウンタ値が格納される（段階１７４）。段階１７６において、第２のホッピングコードが受信される。このコードが復号化され（段階１７８）、復号化された管理コードが格納された管理コードを用いて確認される（段階１８０）。もし値が一致しなければ、学習プロセスは無効であると見なされ、中止(abort)される。次に段階１８２において、カウンタ値が、格納されたカウンタ値を用いて確認される。値が一致しなければ、送信は無効かつ不適正な(illegitimate)学習動作であると見なされ、中止される。カウンタ値が一致すれば、有効な学習動作と見なされる（段階１８４）。通常のコードホッピングシステム動作におけるようにカウンタが一致しない場合、カウンタ同期検査（段階１８２）において若干余裕をもたせ、復号化器によって復号化されなかったかもしれない中間送信を可能にし、これらが一致し有効と見なされたならば容認してもよい。

段階１８４において、有効な学習プロセスが完了したと仮定している。段階１８６において次の学習ポインタ（図３における参照符号１０８）を、次の利用可能な学習位置を指すようにアップデートする。特定の符号化器と関連付けられた出力構成学習を、必要であれば段階１８８において含めてもよい。段階１９０において、学習サイクルは完了する。

明らかに、上記の教示に基づいて、本発明の多くの改変および変形が可能である。例えば、符号化器部１０は、アプリケーション専用集積回路（application specific integrated circuit:ASIC)上に実現される。回路の一部は例えばパラメータセット５６およびオプション７６などの変化するプログラム可能な個々の値を格納するために使用される、不揮発性メモリで構成される。システムのセキュリティおよび実用的な側面を確保するためにこの実現方法が用いられるが、コンピュータまたはマイクロプロセッサコントローラ内のソフトウェアとして実現されてもよい。同じアプローチが復号化器１２に用いられる。機能部およびメモリ部はASIC上に実現されるが、コンピュータまたはマイクロプロセッサコントローラ上で実現されてもよい。この実施態様は、復号化器において好ましくあり得る。なぜなら、多くのユーザがシステムにアクセスすることを可能にするために、復号化器は大量の情報を格納することが要求され得るためである。従って、付属の請求項の範囲内において、本発明は本明細書において具体的に記載された以外にも実施され得ることが、理解される。

【図１】

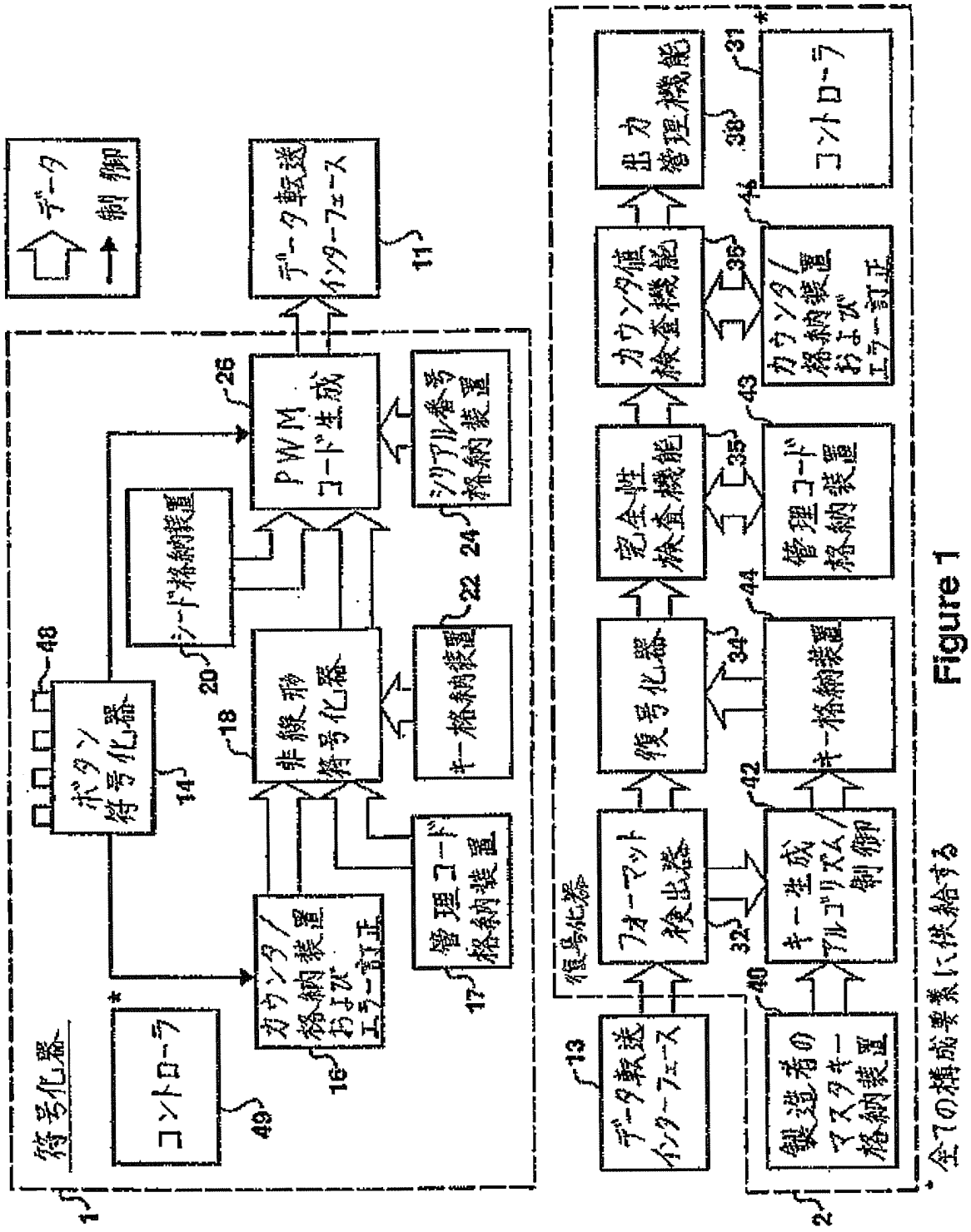

データ
制御
符号化器
コントローラ
ボタン符号化器
カウンタ/格納装置およびエラー訂正
非線形符号化器
キー格納装置
管理コード格納装置
シード格納装置
PWMコード生成
シリアル番号格納装置
データ転送インターフェース
復号化器
データ転送インターフェース
フォーマット検出器
キー生成アルゴリズム制御
製造者のマスターキー格納装置
復号化器
キー格納装置
管理コード格納装置
完全性検査機能
カウンタ値検査機能
カウンタ/格納装置およびエラー訂正
出力管理機能
コントローラ
全ての構成要素に供給する

Figure 1

【図２】

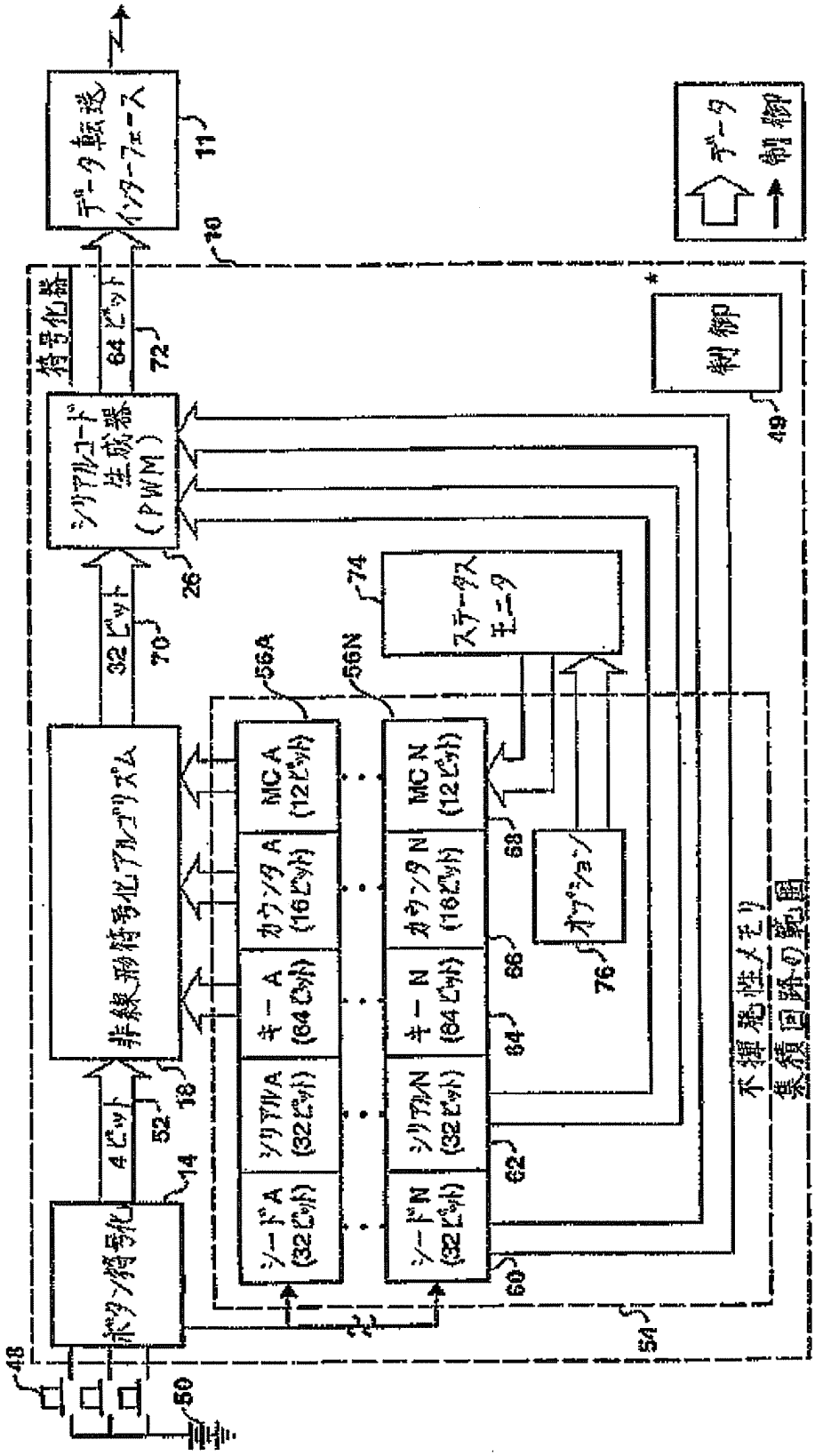

データ転送インターフェース
11
10
符号化器
64ビット
72
シリアルコード生成器（PWM）
26
制御
49
データ
制御
32ビット
70
非線形符号化アルゴリズム
18
4ビット
52
14
ステータスモニタ
74
56A
56N
MC A (12ビット)
MC N (12ビット)
カウンタA (16ビット)
カウンタN (16ビット)
キーA (64ビット)
キーN (64ビット)
シリアルA (32ビット)
シリアルN (32ビット)
シードA (32ビット)
シードN (32ビット)
オプション
76
68
66
64
62
60
54
ボタン符号化
48
50
不揮発性メモリ
集積回路の範囲
*全ての構成要素に供給する

Figure 2

【図３】

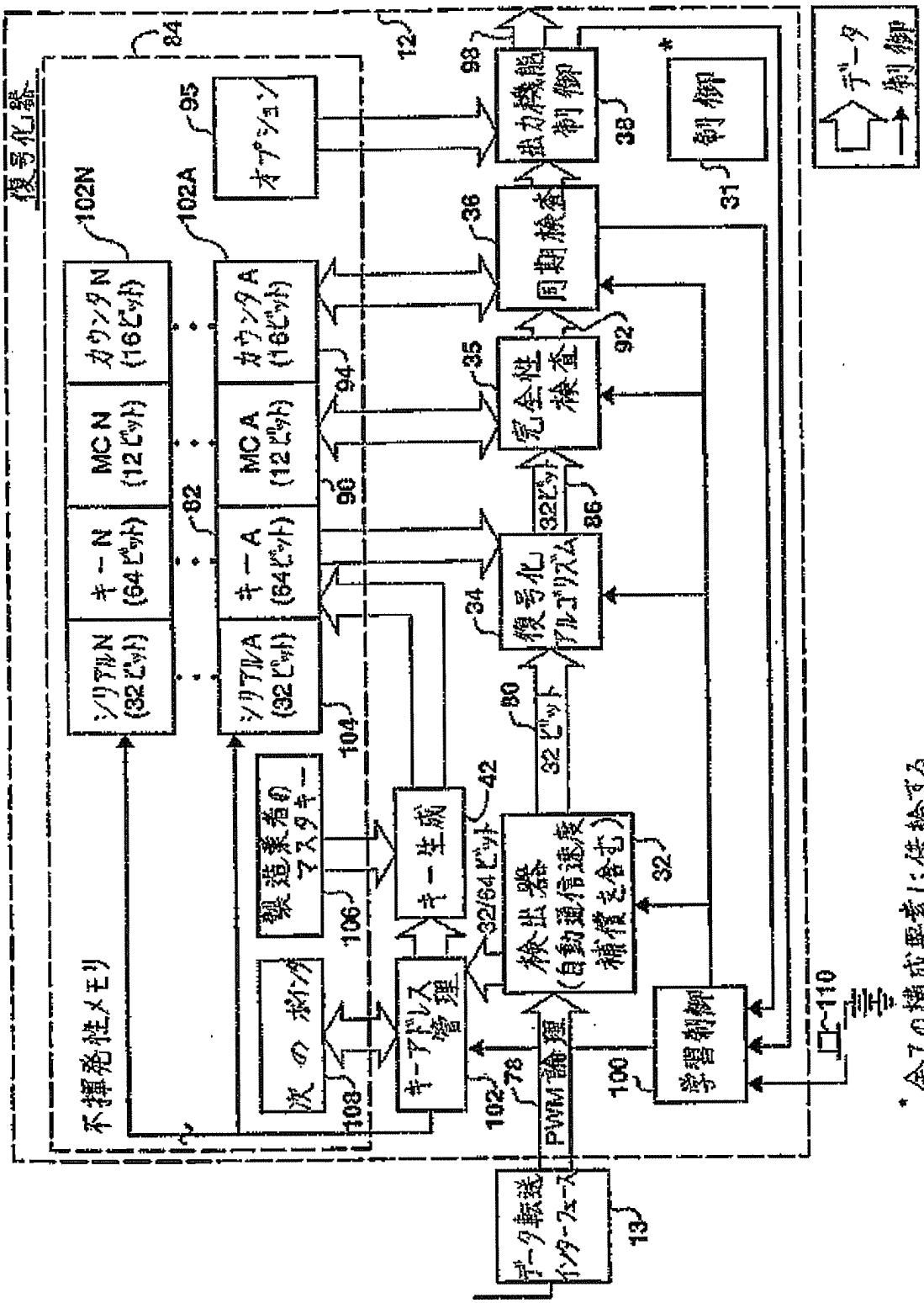

復号化器
84
不揮発性メモリ
シリアルN (32ビット)
キーN (64ビット)
MC N (12ビット)
カウンタN (16ビット)
102N
シリアルA (32ビット)
キーA (64ビット)
MC A (12ビット)
カウンタA (16ビット)
102A
オプション
95
82
104
製造業者のマスターキー
106
次の命令
108
キー生成
42
キーアドレス管理
102
32/64ビット
検出器 (自動通信速度補償を含む)
32
78
PWM論理
32ビット
80
復号化アルゴリズム
34
32ビット
86
完全性検査
35
92
94
96
同期検査
36
出力機能制御
38
12
93
制御
31
データ制御
学習制御
100
110
データ転送インターフェース
13
PWM
*全ての構成要素に供給する

Figure 3

【図４】

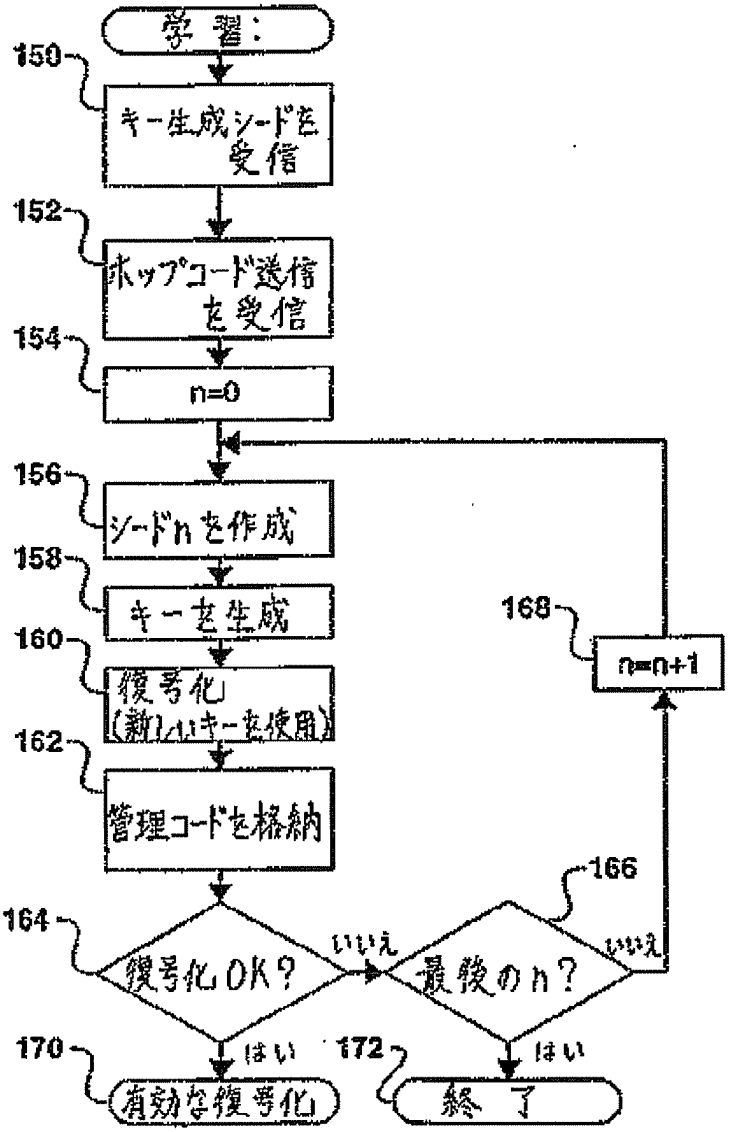

学習：
150
キー生成シードを受信
152
ホップコード送信を受信
154
n=0
156
シードnを作成
158
キーを生成
160
復号化【新しいキーを使用】
162
管理コードを格納
164
復号化OK？
いいえ
166
最後のn？
いいえ
はい
168
n=n+1
はい
170
有効な復号化
172
終了

Figure 4a

【図４】

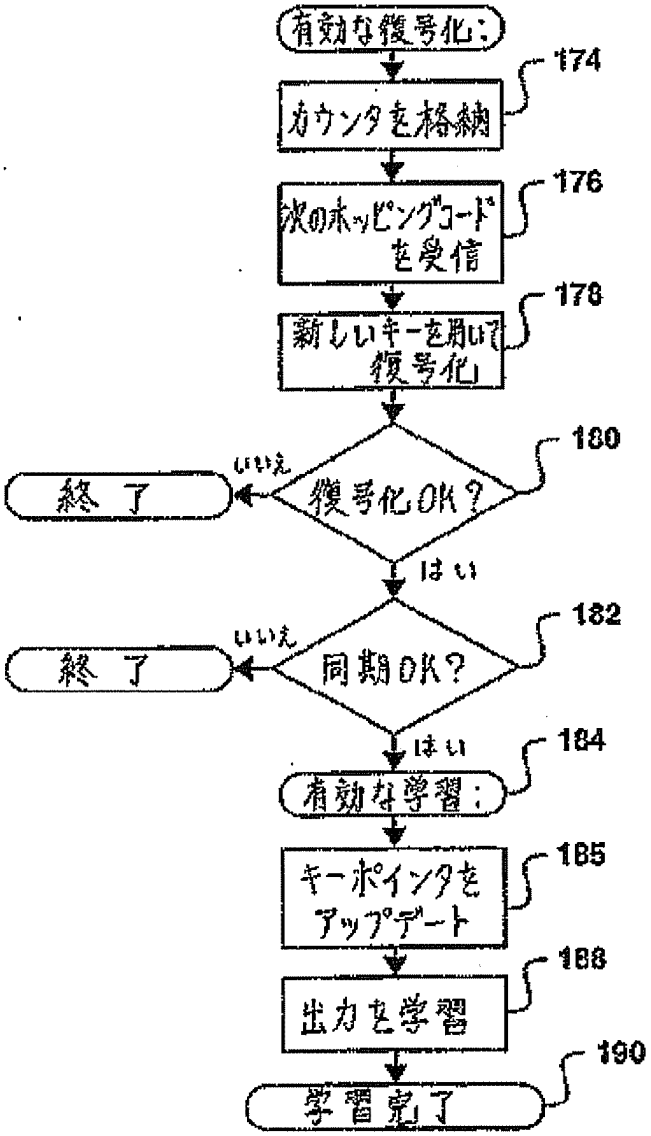

有効な復号化;
174
カウンタを格納
176
次のホッピングコード
を受信
178
新しいキーを用いて
復号化
180
復号化OK?
いいえ
終了
はい
182
同期OK?
いいえ
終了
はい
184
有効な学習;
185
キーポインタを
アップデート
188
出力を学習
190
学習完了

Figure 4b

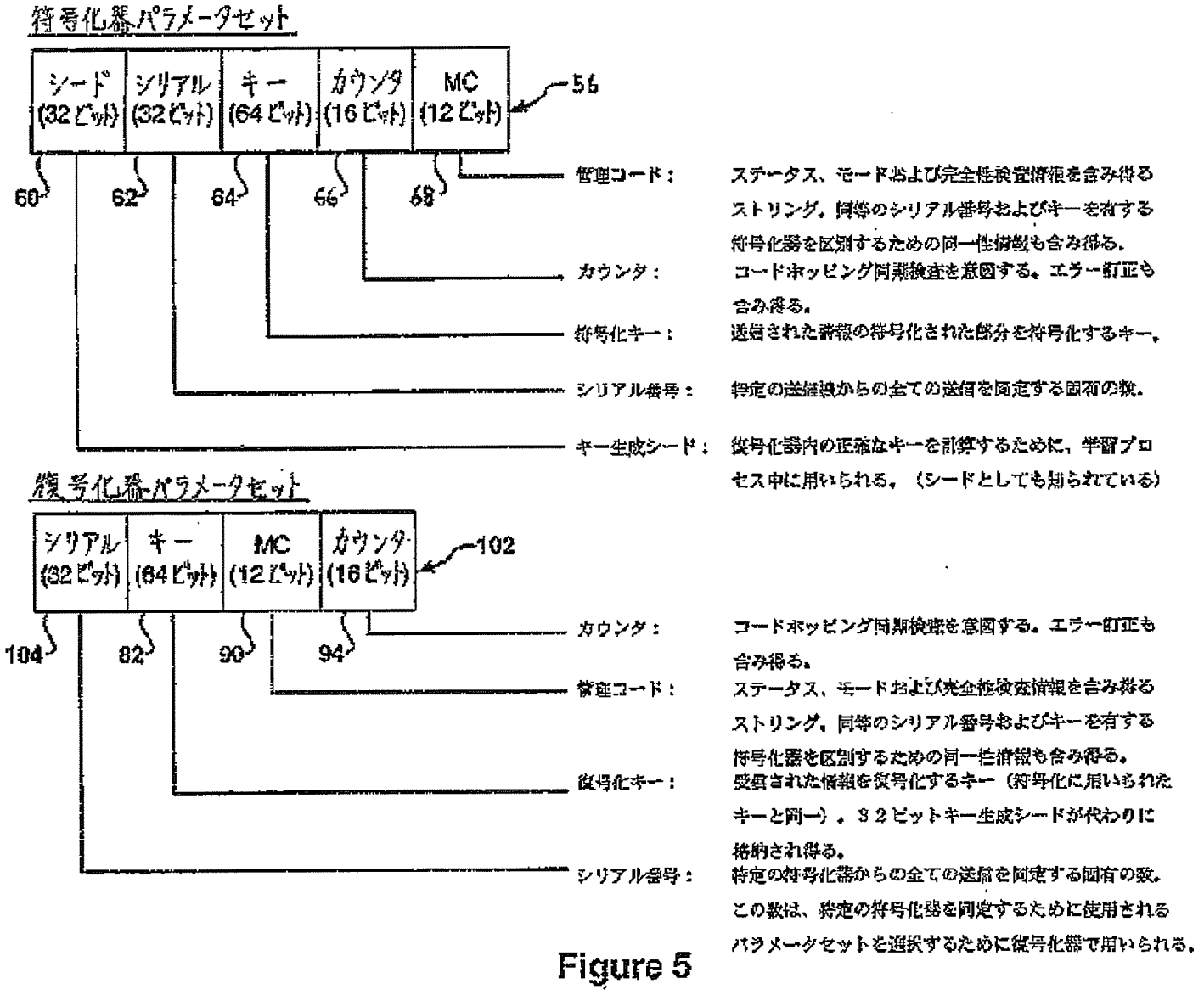


Figure 5

特表２０００－５１６３１３

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 98/11365

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 E05B49/00 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 E05B H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 688 929 A (NANOTEQ (PROPRIETARY) LIMITED) 27 December 1995 see column 3, line 3 - column 30, line 50; figures 1-5	1-5
A	US 5 506 905 A (MARKOWSKI,KHAMHARN,BIANCO) 9 April 1996 see column 3, line 45 - column 5, line 40; figures 1-3	1-3
A	US 5 191 610 A (HILL,FINN) 2 March 1993 see column 5, line 20 - column 8, line 40; figures 3,4	1,2
P,X	US 5 686 904 A (BRUWER) 11 November 1997 see column 2, line 50 - column 22, line 29; figures 1-5	1-5

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 1998	23/10/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax. (+31-70) 340-3016	Herbelet, J.C.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/11365

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 688929	A	27-12-1995	US	5686904 A	11-11-1997
			ZA	9505429 A	13-02-1996
US 5506905	A	09-04-1996	US	5767784 A	16-06-1998
US 5191610	A	02-03-1993	NONE		
US 5686904	A	11-11-1997	US	5517187 A	14-05-1996
			EP	0688929 A	27-12-1995
			ZA	9505429 A	13-02-1996